Segurança, privacidade e anonimato – guia básico

By **Gabriel Camargo** 12/10/2022

Créditos da imagem: Veja

Continuando com a série *Segurança, Privacidade e Anonimato*, neste artigo será dado início aos guias propriamente ditos. O nível primeiramente apresentado será o básico, voltado para aqueles que desejam limitar a quantidade de informações enviadas para as grandes empresas de tecnologia e anunciantes, bem como elevar o nível de segurança digital. Recomenda-se que todos ao menos estejam nesse nível.

Índice

- Internet e Navegadores
- Softwares e aplicativos
- Roteadores
- Smartphones
- Laptop e desktop
- Dicas adicionais

Internet e Navegadores

Senhas

Um hábito comum entre internautas é a reutilização de senhas. Mesmo que seja prático esse hábito pode ter consequências severas. Vazamentos de dados são comuns; todas as semanas novas notícias surgem sobre empresas que publicamente admitiram invasão e roubo de seus dados. Quantas outras nada dizem sobre isso? Nunca saberemos. Empresas grandes como a Uber tentaram impedir que um vazamento em seus bancos de dados se tornasse público, mas claramente isso não ocorreu.

Quando um atacante invade um sistema, principalmente servidores de empresas, ele comumente procura por credenciais. Uma boa prática é o armazenamento de hashs em vez de senhas em formato textual. Mas esse nem sempre é o caso. E mesmo em hash não há garantia de confidencialidade futura, por fraquezas no próprio algoritmo de criptografia ou por ataques de força bruta nos dados por descobrir.

Para a proteção contra esse tipo de ataque, deve-se usar senhas longas (menores que 8 caracteres não valem nada) e únicas para cada conta. Quanto maior a senha, maior a sua entropia e, como consequência, maior será a sua força.

Como é impossível guardar senhas únicas e complexas para todas as contas digitais, utiliza-se um gerenciador de senha. O software recomendado é o KeePassXC. Além de elevar muito o nível de proteção, é possível fazer uma verificação de todas as contas existentes. O usuário também poderá manter apenas as senhas que forem mais úteis para ele. Com o passar do tempo contas antigas e com pouco uso se acumulam; convém deletá-las para a redução da pegada digital. Senhas fortes devem conter letras, números e símbolos. Pode-se também utilizar frases.

Desde que as senhas sejam longas e únicas, o nível de proteção será significativamente elevado. Não se deve utilizar informações pessoais para compor senhas, pois essas informações podem ser conhecidas por pessoas próximas e/ou podem ter sido compartilhadas anteriormente, por exemplo, em redes sociais.

Em todas as contas nas quais essa opção está disponível, convém habilitar a autenticação de duas etapas (2FA). Por meio dela, mesmo que um atacante obtenha sucesso em saber as credenciais do usuário, não poderá acessar a conta. Não é recomendada a autenticação de dois fatores feita por SMS, por ser um método inseguro de comunicação e passível de interceptação por ataques de clonagem de números de celular. Recomenda-

se o uso de aplicativos como o Aegis, no qual os códigos temporários são gerados para completar o processo de login, em uma técnica conhecida como TOTP (Time-basedone-time password).

Alguns ataques utilizam as senhas salvas nos navegadores como fonte de coleta de informação. A praticidade de ter senhas salvas nos navegadores vem com o risco associado de segurança. Novamente, uma prática mais eficaz para a proteção de contas digitais é a utilização de um gerenciador de senhas.

E-mails

No recebimento de e-mails, como medida de prevenção, deve-se evitar clicar em links presentes no corpo das mensagens. Se necessário, o melhor é acessar o site diretamente por um mecanismo de pesquisa. O mesmo vale para mensagens de SMS. Mesmo e-mails com identidade visual convincente podem ser falsos.

Atenção aos detalhes, pois mesmo os bem-feitos geralmente pecam nos detalhes. Pode-se utilizar um serviço de verificação de links, como o Virus Total, para verificar um link antes de clicar, mas esse método não é infalível. Também deve-se tomar cuidado com arquivos enviados em anexo, pois eles podem conter diferentes tipos de malware que comprometerão a segurança do computador.

O Vitus Total também verifica arquivos para a presença de malwares. No entanto, não é recomendado o envio de arquivos com informações pessoais ao serviço, já que os arquivos são compartilhados com os diferentes parceiros do serviço.

Com o tempo, as caixas de entrada das contas de e-mail ficam repletas de informações e mensagens antigas. É uma boa prática deletar as mensagens que não são mais necessárias. Assim, pode-se reduzir a quantidade de informações presentes na conta.

Um dos principais meios de ataque e disseminação de softwares maliciosos são os e-mails. Um exemplo comum são aquelas mensagens de e-mail em tom alarmista, onde se diz que está terminando o prazo de renovação de um serviço, que pode ser do próprio e-mail que está sendo utilizado. A mensagem diz ser necessário clicar em um link e colocar novamente as credenciais para evitar a suspensão dos serviços.

Caso clique no link, o usuário será direcionado para uma página falsa, onde

deverá colocar suas informações de login. Após ter feito isso, é redirecionado para o serviço verdadeiro, sem desconfiar de nada. O que ocorreu contudo, foi que os atacantes agora possuem as informações inseridas na página falsa e, caso não haja proteção por 2FA, poderão entrar na conta e comprometer todas as informações presentes nela.

Ataques mais recentes possuem a capacidade de comprometer a conta do usuário mesmo com a utilização do 2FA, por isso, valem as dicas apresentadas anteriormente. Ainda, para dificultar ataques desse tipo, pode-se utilizar uma hardware key, como a Nitrokey.

É importante saber reconhecer mensagens desse tipo. Uma das formas é por meio dos endereços presentes na barra de navegação. Porém, ataques mais recentes têm se utilizado de endereços parecidos com os originais e criptografia, tornando o cadeado na barra de endereços inútil para verificar se um link é falso ou não.

Deve-se desconfiar de mensagens que peçam algo, como dados pessoais e de login, que tenham teor alarmista ou prometam benefícios caso um link seja clicado. Na dúvida o melhor a fazer é contactar o banco ou o serviço em questão, em vez de clicar nos links do corpo da mensagem.

Contas digitais em geral

Nas redes sociais é uma boa prática pensar antes de postar. Pode parecer estranho, mas postar algo sem pensar pode ocasionar problemas. Deve-se compartilhar apenas o que desejar ser permanentemente conhecido. Revisar o conteúdo das postagens e compartilhamentos deve se tornar uma prática rotineira, com o intuito de não compartilhar informações de forma desnecessária.

Logo de início, após abrir uma conta em um serviço, sendo rede social, conta de e-mail, site de compras, etc., convém procurar pelo menu de configurações e ver quais opções de privacidade e segurança estão disponíveis, como a autenticação de dois fatores e opções para limitar o compartilhamentos de dados com empresas e serviços parceiros.

Navegadores

O navegador é um dos principais softwares instalados nos dispositivos pessoais, sendo um dos principais pontos de contato com o mundo exterior. Extensões adicionam funcionalidade e comodidade aos navegadores. Porém, apenas extensões confiáveis devem ser instaladas, pois adquirem privilégios elevados e criam o ambiente propício para a exploração

maliciosa da navegação. Apenas extensões confiáveis devem ser instaladas e mantidas.

Empresas honestas não são as únicas que criam anúncios digitais (e mesmo a infraestrutura de empresas honestas pode ser comprometida). Sendo assim, propagandas e redes de anúncios comprometidos para a disseminação de malwares são um problema real. Esse tipo de ataque é denominado malvertising, é especialmente difícil de ser detectado por um usuário comum.

Mesmo que o usuário possua bons hábitos de navegação, quando comprometida, uma rede de anúncios pode disseminar malwares aos visitantes de sites legítimos. Utilizar navegadores com bloqueadores integrados, como o Brave Browser, Firefox e LibreWolf, ajudam a mitigar ataques desse tipo, além de elevar o nível de privacidade.

O navegador mais comum da atualidade, por uma grande margem, é o Google Chrome. Contudo, e ainda mais quando logado na conta do usuário, todas as ações executadas no navegador tem o potencial de ser logadas e utilizadas para a criação de um perfil. Recomenda-se utilizar um navegador alternativo para certos tipos de navegação, limitando ao Chrome apenas aquilo que é relacionado ao Google e seus produtos.

Softwares e aplicativos

Recomenda-se um foco minimalista, instalando apenas o que for necessário e removendo aquilo que não serve mais. Cada instalação potencialmente abre uma nova porta de exploração do sistema.

Uma das formas mais diretas de proteger a segurança é manter todos os programas atualizados. Bem como os navegadores. Por meio das atualizações periodicamente fornecidas pelos desenvolvedores, são corrigidas vulnerabilidades que, caso exploradas, podem levar à perda de dados ou infecção por malwares. Muitos ataques realizados contra usuários (e até grandes empresas) exploram vulnerabilidades já conhecidas e corrigidas.

Os danos teriam sido evitados se os sistemas estivessem atualizados. Cada sistema operacional, bem como cada aplicativo, possui opções de atualização ligeiramente diferentes, geralmente na aba ou menu “sobre”. Deve-se verificar e instalar atualizações periodicamente, principalmente as relativas à segurança (as de novas funcionalidades podendo ser deixadas para mais tarde, dependendo dos requisitos do usuário), pelo menos, uma

vez ao mês.

Deve-se dar preferência a aplicativos gratuitos e de código aberto (open source), pois, além de serem gratuitos e muitos serem capazes de realizar funções encontradas em alternativas pagas, por terem seus códigos-fonte abertos e acessíveis, apresentam benefícios de segurança e privacidade a seus usuários.

Roteadores

Os roteadores das companhias provedoras de internet geralmente vêm com credenciais padrão. Essas credenciais devem ser alteradas pelo usuário, com o objetivo de adicionar segurança à rede. Em qualquer navegador de preferência, digita-se o endereço IP do roteador, geralmente, 192.168.0.1, e se insere as credenciais encontradas em uma etiqueta presa ao roteador. Deve-se alterar a senha padrão por uma mais forte.

Um ataque possível, e já executado no Brasil, é o uso de sites comprometidos para tentar acessar o roteador. Sites legítimos comprometidos efetuam tentativas de acesso ao roteador do visitante, por meio das combinações padrão de acesso, como “admin” ou “admin12345”. Com a alteração da senha padrão, mesmo quando o usuário acessa um site comprometido, o código malicioso não conseguirá comprometer a segurança. Ainda no roteador, é uma boa prática desabilitar o WPS e o UPNP quando esses não são necessários, por aumentarem a superfície de ataque.

Smartphones

No celular, deve-se desativar o Bluetooth e a localização quando esses não estiverem em uso ou não forem necessários. Isso pode ser feito facilmente pelo painel que aparece quando se arrasta para baixo a parte superior da tela.

Deve-se ter uma senha forte para entrar no celular. Evite senhas óbvias como “senha” ou “12345”. Opte por algo que impeça alguém de acessar os dados internos quando o usuário não estiver por perto. Não é recomendado o uso de biometria ou identificador de face para desbloquear o dispositivo, pois são maneiras inferiores de efetuar o login com segurança.

Do mesmo modo que no computador, manter os aplicativos atualizados é importante para a segurança do usuário. No aplicativo da loja de

aplicativos, Google Play Store, deve-se clicar no logotipo da conta de usuário, e verificar a existência de atualizações no gerenciamento de aplicativos.

Igualmente ao computador, não se deve deixar muitos arquivos no celular, devendo os arquivos mais antigos ou já sem importância ser excluídos ou transferidos para um backup externo, como um pendrive, cartão de memória, HDD externo ou conta em nuvem. Deve-se tomar cuidado, porém, pois backups com sincronização automática podem, por descuido do usuário, apagar os arquivos que se pensava estarem a salvo. O minimalismo não se limita aos aplicativos instalados, mas a todos os dados armazenados.

Nas configurações do dispositivo, o usuário deve procurar por termos como “permissões”, “aplicativos”, “privacidade”, “criptografia”e “localização”; analisar as opções que surgirem e decidir o que pode ser alterado. Deve-se remover todos os aplicativos que não são necessários ou de muito pouco uso, bem como revisar as permissões concedidas (principalmente de microfone, câmera, contatos e armazenamento) para os aplicativos que permanecerem.

Aplicativos como a calculadora não necessitam de acesso aos contatos, por exemplo. No entanto, deve-se tomar cuidado para não revogar permissões importantes, principalmente em softwares críticos, como o Google Play Services.

Para aplicativos de mensagens, como Whatsapp, Telegram e Signal, deve-se habilitar o PIN para elevar o nível de proteção da conta. Assim como com todas as outras contas e serviços, deve-se analisar as configurações desses aplicativos e verificar as opções de privacidade disponíveis.

Por fim, dispositivos desbloqueados não devem ser deixados sozinhos, principalmente em ambientes públicos. Também deve ser evitado andar na rua enquanto o celular estiver em uso, pois, como ele estará destrancado, aquele que o roubar poderá ter acesso a tudo o que estiver armazenado, incluindo contatos e contas em bancos digitais.

Laptop e desktop

Para tornar o Windows um sistema operacional mais privado, na caixa de pesquisa do menu inicial, procure por “Serviços”. Encontre, pare e desative o serviço “Experiências do Usuário Conectados a Telemetria”.

Na caixa de pesquisa, procure por “Agendador de Tarefas”. Siga o caminho:

Biblioteca do Agendador -> Microsoft -> Windows -> Application Experience. Desative todas as tarefas agendadas. Ainda em “Windows”, desative as tarefas encontradas em “Customer Experience Improvement Program”.

Por fim, novamente na caixa de pesquisa do menu inicial, procure por “Regedit”. Siga o caminho: HKEY_LOCAL_MACHINE -> SOFTWARE -> Policies -> Microsoft -> Windows -> DataCollection. Clique com o botão direito do mouse e crie um novo valor DWORD 32-bit. Nomeie-o como “Allow Telemetry” e coloque o valor como 0. Reinicie o computador.

Para remover a Cortana no PowerShel, digite o comando:Get-AppxPackage -allusers Microsoft.549981C3F5F10 | Remove-AppxPackage

No menu iniciar analise os aplicativos instalados e pratique o minimalismo. Não é recomendado o uso rotineiro de contas com privilégio de administrador, pois isso abre consideráveis possibilidades para malwares infectarem e danificarem o dispositivo. Também não é recomendado o uso de uma conta de usuário sincronizada com a conta da Microsoft. Crie uma nova conta local e sem esses privilégios.

Ao abrir as configurações, clique nas opções de privacidade e segurança. Analise todas as opções presentes nesse menu, desabilitando aquilo que não for necessário. Nos dispositivos com MacOS, procure nas preferências do sistema o menu “Segurança e Privacidade”.

Caso utilize seu laptop em redes públicas ou em diferentes localidades com frequência, procure no mesmo painel de configurações as opções de rede e internet e, em Wi-Fi, habilite a randomização do endereço MAC.

Utilize o antivírus nativo do sistema, Windows Defender. No entanto, convém desabilitar a submissão automática de arquivos. Essa opção pode ser encontrada no painel de segurança do sistema, na aba de proteção contra vírus e ameaças. O uso de outros programas antivírus ou antimalwares não é recomendada. Seguindo as orientações desta série, você obterá um nível elevado de proteção contra ameaças digitais.

Esse tipo de software não é eficaz contra ameaças sofisticadas, além de introduzir vulnerabilidades no sistema por sua posição privilegiada. O uso de antivírus como portas de entrada de ameaças é comum. E com certeza continuará sendo no futuro.

Utilize senhas fortes para as suas contas de usuário. Não utilize biometria

para acessar sua conta.

Dicas adicionais

- Em todas as suas contas digitais, revise as opções de privacidade e segurança. Exemplos são os painéis das contas do Google e Microsoft, acessadas pelos links abaixo.
- https://myaccount.google.com/
- https://account.microsoft.com/account/privacy
- A opção de pagamento por aproximação de cartões de crédito/débito deve ser desativada, pois pagamentos por aproximação não necessitam de senha. Carteiras comuns não são capazes de impedir o vazamento das frequências utilizadas para efetuar a transação fraudulenta. Uma alternativa é utilizar carteiras ou protetores que bloqueiam radiação eletromagnética, como faraday bags.
- Como cada novo dispositivo é um novo potencial risco à segurança e privacidade, deve-se limitar o número de dispositivos de Internet das Coisas (IOT) presentes em uma residência.
- Deve-se limitar o compartilhamento de informações com parentes, amigos, vizinhos e outros conhecidos, como cabeleireiros e manicures. A partir do momento que as informações são compartilhadas, elas não estarão mais sob o seu controle.
- Evite realizar o download de aplicativos e softwares de fontes duvidosas, ou em versão pirata.
- Deve-se evitar o acesso frequente a redes Wi-Fi públicas, por abrirem possibilidades de comprometer a segurança e privacidade do usuário. Nesse tipo de rede, para a proteção, utilize VPNs confiáveis.
- É recomendado possuir mais de um endereço de e-mail para compartimentalizar a vida digital. Pode-se, por exemplo, possuir um e-mail exclusivamente para compras digitais e outro para assuntos de trabalho e estudo. Assim, além de reduzir as incomodações por spam, caso uma das contas seja comprometida, a outra permanecerá em segurança (caso as outras dicas desse guia tiverem sido seguidas).
- As comunicações por e-mail não apresentam privacidade como as efetuadas por meio de aplicativos criptografados ponta-a-ponta. Evite utilizar e-mails para assuntos sensíveis ou privados, como para o envio de informações para imposto de renda e contabilidade.

Artigo escrito por Gabriel Camargo e revisado por @rodrigo

Tecnologia